APPENDIX II
COMSEC BRIEFING

A. You have been selected to perform duties which will require access to sensitive COMSEC information. It is, therefore, essential that you are made fully aware of certain facts relative to the protection of this information before access is granted. This briefing will provide you with a description of the types of COMSEC information you may have access to, the reasons why special safeguards are necessary for protecting this information, the directives and rules which prescribe those safeguards, and the penalties which you will incur for willful disclosure of this information to unauthorized persons.

B. COMSEC equipment and keying material are especially sensitive because they are used to protect other sensitive information against unauthorized access during the process of communicating that information from one point to another. Any particular piece of COMSEC equipment, keying material, or other cryptographic material may be the critical element which protects large amounts of sensitive information from interception, analysis, and exploitation. If the integrity of the COMSEC system is weakened at any point, all the sensitive information protected by that system may be compromised; even more damaging, this loss of sensitive information may never be detected. The procedural safeguards placed on COMSEC equipment and materials, covering every phase of their existence from creation through disposition, are designed to reduce or eliminate the possibility of such compromise.

C. Communications Security (COMSEC) is the general term used for all steps taken to protect information of value when it is being communicated. COMSEC is usually considered to have four main components: Transmission security, physical security, emission security, and cryptographic security. Transmission security is that component of COMSEC which is designed to protect transmissions from unauthorized intercept, traffic analysis, imitative deception and disruption. Physical security is that component of COMSEC which results from all physical measures to safeguard cryptographic materials, information, documents, and equipment from access by unauthorized persons. Emission security is that component of COMSEC which results from all measures taken to prevent compromising emanations from cryptographic equipments or telecommunications systems. Finally, cryptographic security is that component of COMSEC which results from the use of technically sound cryptosystems, and from their proper use. To ensure that telecommunications are secure, all four of these components must be considered.

D. Part of the physical security protection given to COMSEC equipment and materials is afforded by the special handling it receives for distribution and accounting. There are two separate channels used for the handling of such equipment and materials: "COMSEC channels" and "administrative channels." The COMSEC channel, called the COMSEC Material Control System (CMCS) is used to distribute accountable COMSEC items such as keying material, maintenance manuals, and classified and CCI equipment. (EXCEPTION: Some Military Departments have been authorized to distribute CCI equipment through their standard logistics system.) The CMCS channel is composed of a series of COMSEC accounts, each of which has an appointed COMSEC Custodian who is personally responsible and accountable for all COMSEC materials charged to the account. The COMSEC Custodian assumes responsibility

for the material upon receipt, and then controls its dissemination to authorized individuals on a need-to-know basis. The administrative channel is used to distribute COMSEC information and materials other than that which is accountable in the COMSEC Material Control System.

E. Particularly important to the protection of COMSEC equipment and materials is an understanding of all security regulations and the timely reporting of any compromise, suspected compromise, or other security problem involving these materials. If a COMSEC system is compromised but the compromise is not reported, the continued use of the system, under the incorrect assumption that it is secure, can result in the loss of all information that was ever protected by that system. If the compromise is reported, steps can be taken to change the system, replace the keying material, etc. , to reduce the damage done. In short, it is your individual responsibility to know and to put into practice all the provisions of the appropriate publications which relate to the protection of the COMSEC equipment and materials to which you will have access.

F. Public disclosure of any COMSEC information is not permitted without the specific approval of your Government contracting office representative or the National Security Agency (NSA). This applies to both classified and unclassified COMSEC information, and means that you may not prepare newspaper articles, speeches, technical papers, or make any other "release" of COMSEC information without specific Government approval. The best personal policy is to avoid any discussions which reveal your knowledge of or access to COMSEC information and thus avoid making yourself of interest to those who would seek the information you possess.

G. Finally, you must know that should you willfully disclose or give to any unauthorized persons any of the classified or CC1 COMSEC equipment, associated keying materials, or other classified COMSEC information to which *you* have *access,* you will be subject to prosecution under the criminal laws of the United States. The laws which apply are contained in Title 18, United States Code, sections 641, 793, 794, 798, and 952.

H. If your duties include access to classified COMSEC information, in addition to the above, you should avoid travel to any countries which are adversaries of the United States, or to their establishments/facilities within the U.S. Should such travel become necessary, however, your security office must be notified sufficiently in advance so that you may receive a defensive security briefing. Any attempt to elicit the classified COMSEC information you have, either through friendship, favors, or coercion must be reported immediately to your security office.